COCOM Cyber Mission Support (CCMS)
Performance Based Statement of Work (PBSOW)

C.1 BACKGROUND

This effort provides the Department of Defense (DoD) and its interagency partners with research, development, test and evaluation, operations, maintenance, and training capabilities and related professional services that will meet dynamic capability development requirements.

C.1.1 PURPOSE

The purpose of this TO is to provide the DoD, Combatant Commands (COCOMs), services, and its interagency partners with research, development, test and evaluation, operations, maintenance, and training capabilities, cyber capability and tools development, advanced concepts support, data analytics, and related professional services. This initiative will rapidly provide capabilities and development services through collaboration with Government and industry partners and will assist in developing and strengthening Cyberspace Operations (CO) capabilities for operational forces.

C.2 SCOPE

The scope of this requirement is to provide DoD strategic and portfolio management support across space, ground, air, maritime and cyberspace domains by leading Alternatives Analysis (AoAs) for future state capabilities and emerging technologies. This requirement supports system integration across DoD domains, synchronizing communication architectures, C2, and cyber capabilities. Furthermore, this requirement provides prototyping and experimentation of emerging technologies; vulnerability, security, data analytics support, and market research within DoD and commercial technology space; and concept test out through training, exercise support and scenarios to DoD end users.

C.3 OBJECTIVE

Specific objectives of this TO include:

- Vulnerability, security, data analytics support, and market research within DoD designated technologies and concepts;
- Creation, integration, operation, and maintenance of cyber development and experimentation environments, and conducting cyber experimentation for advanced capability and analytic support concepts;
- Development, delivery, and maintenance of CO infrastructures, networks, platforms, capabilities, tools, and systems;
- Development and execution of quality control processes to include informal and formal Test and Evaluation (T&E) and documentation;
- Development and implementation of training and exercise environments, systems, documentation, and scenarios for DoD designated end users;
- Operational support for fielded capabilities in support of ongoing priority efforts

C.4 TASKS

RSC-NCR priorities are heavily contingent on activity which is primarily driven by war, terrorism, and/or threat situations and can change depending on the nature of intelligence received. As the global dynamics shift and U.S. priorities within the cyber mission areas shift, the contractor must adapt. The following tasks are intended to cover the scope of work that RSC-NCR anticipates for CCMS. Specific work products within the work scope may shift based on our Mission partner needs. Specific work products will be assigned by RSC-Mission Partners through the issuance of Technical Direction (TD) letters.

Below is a summary of the Tasks associated with Section C.

a. Task 1 – Provide Program Management
b. Task 2 – Research, Development, Test, And Evaluation
c. Task 3 – Operations, Maintenance, And Training

C.4.1 TASK 1 – PROJECT MANAGEMENT

The contractor shall provide project management support under this effort. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Statement of Work (SOW). The contractor shall identify a Program Manager (PM) by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of this contract.

C.4.1.1 SUBTASK 1 –PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at the location approved by the Government (Section F, Deliverable 02). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the contract. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key Personnel, other contractor personnel, representatives from the directorates, other relevant Government personnel, the COR, and the Government Task Manager (GTM).

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (Section F, Deliverable 01) for review and approval by the COR and the GTM prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of contact (POCs) for all parties
b. Draft Project Management Plan (PMP) (Section F, Deliverable 07) and discussion including schedule, tasks, etc.
c. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government)
d. Staffing Plan and status
e. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs))
f. Invoicing considerations
g. Transition discussion

h. Final Baseline Quality Control Plan (QCP) (Section F, Deliverable 12)

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present, as electronic delivery.

The contractor shall draft and provide a Kick-Off Meeting Minutes Report (Section F, Deliverable 03) documenting the Kick-Off Meeting discussion and capturing any action items.

C.4.1.2 SUBTASK 2 – MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide MSRs (Section F, Deliverable 04), each of which shall include the following:

a. Activities during reporting period, by task (include on-going activities, new activities, and activities completed, and progress to date on all above mentioned activities). Each section shall start with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearance, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for monthly reporting period).
g. Accumulated invoiced cost for each CLIN up to the previous month.
h. Projected cost of each CLIN for the current month.
i. Achieved performance against QASP/QCP metrics to date.
j. Classified addendum, as required.
k. Supplemental reporting, per C.4.1.7. (Section F, Deliverable 14)

C.4.1.3 SUBTASK 3 – MONTHLY TECHNICAL STATUS MEETING

The contractor PM shall convene a monthly Technical Status Meeting with the GTM, COR, and other Government stakeholders (Section F, Deliverable 05). The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting (Section F, Deliverable 06).

C.4.1.4 SUBTASK 4 – PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The contractor shall provide the Government with a draft PMP (Section F, Deliverable 07) on which the Government will make comments. The final PMP (Section F, Deliverable 08) shall incorporate the Government's comments. PMP updates (Section F, Deliverable 09) shall be provided as changes occur.

The PMP shall:

a. Describe the proposed management approach.
b. Contain Standard Operating Procedures (SOPs) for all tasks.
c. Include milestones, tasks, and subtasks required in this contract.
d. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.
e. Describe in detail the contractor's approach to risk management under this contract.
f. Describe in detail the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor and the Government.
g. Include the contractor's Baseline QCP.

C.4.1.5 SUBTASK 5 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted (Section F, Deliverable 10). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and Point of Contact (POC) at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained.

C.4.1.6 SUBTASK 6 –QUALITY CONTROL PLAN (QCP)

The contractor shall develop a draft QCP (Section F, Deliverable 11), and deliver a final baselined QCP (Section F, Deliverable 12). The contractor shall periodically update the QCP, as required in Section F (Section F, Deliverable 13), as changes in program processes are identified.

Within the QCP, the contractor shall identify its approach for providing quality control in meeting the requirements of the contract. The contractor's QCP shall describe its quality control methodology for accomplishing contract performance expectations and objectives. The contractor shall fully discuss its validated processes and procedures that provide high quality performance for each Task Area. The QCP shall describe how the processes integrate with the Government's requirements.

C.4.1.7 SUBTASK 7 – FINANCIAL MANAGEMENT

The contractor shall provide financial reporting by cost element and include subcontractor financial data (Section F, Deliverable 14). The contractor shall provide supplemental reporting including: resource planning; cost reporting; impacts assessments; invoicing; and disclosure requirements (Section F, Deliverable 15).

C.4.1.8 SUBTASK 8 – PRESENTATION MATERIALS

The contractor shall conduct presentations and participate in, or provide material for, meetings at times and places to be determined with the Government and contractor. Presentation material shall be due within five (5) days after the presentation (Section F, Deliverable 16).

C.4.1.9 SUBTASK 9 -TRANSITION-OUT

The contractor shall provide Transition-Out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the contract. The contractor shall provide a draft Transition-Out Plan within six months of Project Start (PS) (Section F, Deliverable 17). The Government will work with the contractor to finalize the Transition-Out Plan (Section F, Deliverable 18) in accordance with Section E. At a minimum, this Transition-Out Plan shall be reviewed and updated NLT 90 calendar days prior to expiration of the TO (Section F, Deliverable 19).

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes
b. Points of contact
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor to contractor coordination to ensure a seamless transition
f. Transition of Key Personnel
g. Schedules and milestones
h. Actions required of the Government

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless Transition-Out.

The contractor shall implement its Transition-Out Plan NLT three months prior to expiration of the contract (Section F, Deliverable 20).

C.4.1.10 SUBTASK 10 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the *US Army* via a secure data collection site. The contractor shall completely fill in all required data fields using the following web address: http://www.ecmra.mil/ (Section F, Deliverable 21).

Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the support desk at: http://www.ecmra.mil/.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.4.2 TASK 2 – RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

The contractor shall research, develop, test and evaluate tailored cyber solutions and capabilities for CO, advanced CO concepts and technologies and integrated operational platforms. Focusing on cyberspace objectives, the contractor shall research and develop technical capabilities for operational use that provide DoD with a significant advantage in cyberspace superiority. Capabilities include unifying and integrating operational platforms, accelerating research and development into leap-ahead technologies to defend US interests in cyberspace, and assessing the Cyber Mission Force (CMF) agility when confronted with multiple contingency outcomes. The contractor shall develop rapid prototypes in direct support to CO performed by the operational users. The contractor shall use reverse engineering, vulnerability research, modeling, and/or simulation to provide access and exploitation development and application development for software, systems, and analytics under this task.

Specifically, the contractor shall provide support to:

a. Develop tailored CO solutions and capabilities to secure, exploit, and analyze cyber for the Sponsor;
b. Research, identify, and analyze potential cyber solutions that advance current cyber operational concepts and/or technologies;
c. Provide expert systems engineering based recommendations on emerging, supporting, and/or related cyber technologies;
d. Integrate CO capabilities within system-of-system concepts.

C.4.2.1 SUB TASK 1 – VULNERABILITY RESEARCH

As required due to a changing threat environment, the Contractor shall provide Vulnerability Research (VR) of Sponsor designated software and hardware systems (to be provided as GFI at contract award and at appropriate program management milestones). This task requires the contractor to research systems to determine vulnerabilities in order to better enable user's freedom of operation within cyberspace. VR shall include identification and mitigation tactics and techniques for use against adversary attack vectors and in Intelligence, Surveillance, and Reconnaissance (ISR) analytics and tools. VR shall lend itself to increased situational awareness (SA) within the CO domain and be employable in modeling and simulation, and other supporting services.

C.4.2.2 SUB TASK 2 – SECURITY RESEARCH

The Contractor shall provide security research of COCOM and assigned and allocated service designated software and hardware systems. The contractor shall:

a. Research and implement Information Assurance (IA) technologies, tactics, and techniques to mitigate external and insider risks to the use, processing, storage, and transmission of data and information
b. Research of innovative cryptographic models for authentication, authorization, and encryption for data and information security
c. Research of CO attribution strategies; and research/data analytical models for non-repudiation.

The contractor shall include in their research an IA technologies ability to ensure maximum availability, integrity, authentication, confidentiality, and non-repudiation of data and information are maintained.

C.4.2.3 SUB TASK 3 – MARKET RESEARCH

The Contractor shall perform and provide market research of cyber technologies to track, understand, and evaluate technology evolutions, market trends and patterns. This includes the following scope of topics:

a. Broad scope cyberspace research and analysis

b. Analysis of known cyber threats

c. Research and assessment of new and emerging technologies within Sponsor designated research areas.

C.4.2.4 SUB TASK 4 – MALWARE ANALYSIS

As required due to a changing threat environment, the Contractor shall provide malware analysis, countermeasure assessment, and capability development support to include the following activities:

a. Identify new exploits and security vulnerabilities, analyze behavior of malicious code, research open source data, document host/network signatures, and develop mitigation and remediation strategies leveraging analytic models;

b. Compile data sets in order to perform dynamic and static analysis and reverse engineering of malware artifacts;

c. Develop, archive, and maintain findings in technical analysis and recommendation reports;

d. Support the release of analytics and technical reports by the Government;

e. Examine media and malware analysis reports and operational reporting from DoD incidents to correlate similar events, tradecraft, and TTPs of malicious activity. Develop, archive, and maintain analytics in support of operational assessments and reporting;

f. Conduct analysis on the lifecycle of adversary anatomy of attack and exploitation and the associated tools, malware, and encryption mechanisms utilized. Develop, archive, and maintain analytics in support of operational assessments and reporting.

C.4.2.5 SUB TASK 5 – INFRASTRUCTURE DEVELOPMENT

The Contractor shall provide cyber infrastructure development and support. The contractor shall develop hardware infrastructure, virtualization infrastructure, and communications infrastructure in support of the COCOM and assigned and allocated service objectives.

The contractor shall ensure that all development tasks will follow designated sponsor processes for requirements review and analysis; design and development; verification; and

test case. The contractor shall perform scenario development to ensure that the user's Concept of Operations (CONOPS) is fulfilled by the infrastructure. The contractor shall provide design results, artifacts, and documentation generated throughout the development process, resulting in an infrastructure development plan (Section F, Deliverable 23).

C.4.2.6 SUB TASK 6 – PLATFORM DEVELOPMENT

The Contractor shall provide platform development and support. The contractor shall develop cyber Command and Control (C2) platforms; resource provisioning and monitoring platforms; operational planning tools and dashboards; and data processing, analysis, and visualization platforms for enabling ISR and Situational Awareness (SA) of the cyber area of operation.

The contractor shall ensure that all development tasks follow the Sponsor's designated process for requirements review and analysis; design and development; verification; and test case and scenario development to ensure that the user's CONOPS is fulfilled by the platform. Results, artifacts, and documentation generated throughout the development process shall be provided at the Sponsor's request (Section F, Deliverable 24).

C.4.2.7 SUB TASK 7 – CAPABILITY DEVELOPMENT

The Contractor shall provide cyber capability tool development and support to ensure that technologies, services and other capabilities are both manageable and streamlined to their full extent. This task includes the development of full spectrum cyber capabilities to include software and hardware systems; sensors; data processing and analytic capabilities; cyber tools; and Sponsor designated emerging technologies and innovations.

The contractor shall ensure that all development tasks follow the Sponsor's designated process for requirements review and analysis; design and development; verification; and testing. The contractor shall provide scenario development to ensure that the user's CONOPS is fulfilled by the capability. Results, artifacts, and documentation generated throughout the development process shall be provided at the Sponsor's request (Section F, Deliverable 25).

C.4.2.8 SUB TASK 8 – INTEGRATION AND INTEROPERABILITY

The Contractor shall provide integration of developed cyber capabilities within the operational cyberspace environment, infrastructure, platforms, and capabilities.

This integration includes integration between Sponsor designated capabilities from the open source community, 3rd party Contractors, Other Government Agencies (OGA), and existing operational capabilities within the COCOM and/or assigned or allocated service environment.

The contractor shall provide support to all necessary preparation activities and after action activities performed to ensure continuity of knowledge and support throughout the lifecycle of the operational capabilities. Specific preparation support shall include the following:

a. logistics and planning activities

b. technical preparation

c. objective preparation (rehearsal, dry run etc.).

Post-support activities shall include providing detailed After Action Reviews (AAR) between technical staff, management, and the customer (Section F, Deliverable 26) Additionally, the Contractor shall provide technical documentation and reports to ensure continuity of knowledge for future support and integration activities (Section F, Deliverable 27).

C.4.2.9 SUB TASK 9 – TEST AND EVALUATION

The Contractor shall perform test and evaluation activities and provide analysis and reporting of these activities. (Section F, Deliverable 28) Specifically, the contractor shall perform the following activities:

a. Provide automated test frameworks for the rapid verification of developed software; including policy and process assessments
b. Conduct T&E planning and preparation activities; including modeling and simulation tools and supporting analytics
c. Develop test plans, test cases, test procedures, and detailed results documents. Develop, archive, and maintain analytics in support of operational assessments and reporting
d. Conduct test and evaluation activities in accordance with Army and DoD testing and evaluation standards, collect and maintain results data, analyze data, and develop new processes and procedures to make existing test procedures more effective and relevant to mission requirements
e. Perform Developmental Testing (DT)
f. Perform Operational Testing (OT)
g. Perform Forensic Analysis and Characterization Testing (FACT);
h. Compile evidence data and reports in support of 3rd party Elevated Level of Assurance (ELA)
i. Conduct penetration testing of hardware and software systems and collect, maintain, and analyze collected data
j. Assess system security policies against client policies, identify system policies that are out of compliance with security requirements, provide recommendations and remediation of compliance failures
k. Conduct cyber capability vulnerability assessments customized to the system function and technical requirements to determine weaknesses and methods of exploitation that may result from improper system configuration, hardware or software flaws, or operational weaknesses
l. Develop and deliver security findings with an assessment of their impact and a recommendation for remediation

C.4.3 TASK 3 – OPERATIONS, MAINTENANCE, AND TRAINING

The Contractor shall provide maintenance and training support of CO technologies and capabilities. This includes providing support for the refresh of operational technologies, providing system engineering and hardware/software/system administration, providing support

and training for Information Assurance best practices, and providing support for formal accreditation processes.

C.4.3.1 SUB TASK 1 – OPERATIONS SUPPORT

The Contractor shall provide operational support for developed CO capabilities in support of the operational forces, to include Cyber Mission Force (CMF), National Mission Force (NMF), Cyber Protection Force (CPF), and Cyber Support teams. The contactor shall provide both on-call as well as on-site personnel support for developed CO capabilities.

The Contractor shall support the development, review, and testing of Tactics, Technique, and Procedures (TTP) in support of CO operations

The Contractor shall support interoperability testing and integration between developed cyber capabilities to enable joint CO objectives.

C.4.3.2 SUB TASK 2 – MAINTENANCE

The Contractor shall provide maintenance and refresh of cyber infrastructures, platforms, and capabilities that have matured beyond the R&D phase. This task includes the continuous upkeep of the following items:

a. Source code repositories
b. Build artifacts
c. Executables
d. Data repositories
e. Test environments
f. Hardware infrastructure

The contractor shall provide knowledgeable development staff for maintenance support to ensure that the Contractor shall respond with rapid technical solutions for fielded products.

The Contractor shall provide hardware infrastructure, virtualization, data repositories, networking, embedded system, and software application administration support in accordance with mission requirements.

Specifically, the contractor shall provide support to the following activities:

a. Operate, maintain, identify, and manage risks to Government information systems to include new technical information systems solutions (both physical and virtual)
b. Develop, maintain, and refresh [cloud-based] proprietary information systems and obtain appropriate Government approval prior to implementing new technical information systems solutions (both physical and virtual)
c. Maintain operating systems and refer/coordinate/interact with the appropriate Government employees or other Contractors to maintain applications
d. Develop, maintain, and refresh network drawings and document configuration information
e. Develop, implement and document system updates, patches and configuration changes

f. Respond to exercise, crisis, or contingency situations by providing system support and systems administration of Government IT assets both hardware and software

g. Test, evaluation, and delivery of updates to capabilities

h. Configure, troubleshoot, and maintain hardware devices required to maintain an operational and secure infrastructure

i. Configure, upgrade, troubleshoot, diagnose, test, monitor, and document operating systems, COTS/GOTS software applications and other various procured software

j. Repair and/or resolve hardware issues, which may require travel to and from remote buildings

k. Coordinate the repair of hardware devices covered by OEM warranties to include performing initial diagnostics, contacting/escorting Contractors, and arranging for receipt and return of equipment

l. Document the work completed in accordance with existing technical writing and system documentation requirements

The contractor shall provide support for and communication of feedback, lessons learned, and operational requests from the end users. All maintenance activities performed under this task shall be prioritized and executed with direction provided by the Sponsor.

C.4.3.3 SUB TASK 3 – TRAINING SUPPORT

The Contractor shall provide training to include cyber operations tool and technique training; on-demand operator training for requested cyber capabilities; User Training (UT) for capabilities undergoing the formal testing process; train the trainer activities; interactive training tool and module development; exercise preparation training; and integration training between capability stakeholders. All training support shall include the development and delivery of documentation, presentations, visualizations, and other training coursework (Section F, Deliverable 30) Where possible, training activities will leverage lessons learned and customer feedback to supplement the offering with content tailored to the end user or trainee (estimated at 30 users per quarter, via a mix of in-classroom and distance learning).

C.4.3.4 SUB TASK 4 – EXERCISE SUPPORT

The Contractor shall provide cyber exercise support and conduct assessments of technologies in collaboration and coordination with the Sponsor, other support Contractors, end users, and other stakeholders (both internal and external).

The Contractor shall provide the following cyber exercise support:

a. Provide logistics, planning, and coordination support to the exercise;

b. Design and develop the exercise scenarios and mission objectives to test the efficiencies of the developed cyber capabilities, mission workflows, and organizational processes;

c. Support the site survey, site preparation, and hardware setup of the exercise environment;

d. Integrate infrastructures, platforms, and capabilities and ensure interoperability with exercise partners and their connected systems for conducting the exercise;

e. Provide on-site personnel support and Subject Matter Expertise (SME) for the execution of the exercise objectives;

f. Provide white team, red team, and blue team services as required by the exercise

g. Develop and maintain exercise analytics and data to prepare, update, and deliver feedback reports describing findings, assessments, impacts, recommended scenario modifications, and lessons learned

DEL. #	MILESTONE/ DELIVERABLE	PWS REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS*
	Project Start (PS)		At TOA	N/A
01	Kick-Off Meeting Agenda	C.4.1.1	NLT 3 workdays prior to Kick-Off Meeting	UR
02	Kick-Off Meeting	C.4.1.1	Within 25 workdays of TOA	N/A
03	Kick-Off Meeting Minutes Report	C.4.1.1	5 workdays of Kick-Off Meeting	UR
04	Monthly Status Report	C.4.1.2	Monthly, 10th calendar day of the next month	UR
05	Monthly Technical Status Meeting	C.4.1.3	Monthly, at mutually agreed upon calendar day of the month.	N/A
06	Monthly Technical Status Meeting Minutes	C.4.1.3	5 workdays of Monthly Technical Status Meeting	UR
07	Draft Project Management Plan	C.4.1.4	Due at Kick-Off Meeting	UR
08	Final Project Management Plan	C.4.1.4	10 workdays after receipt of Government comments	UR
09	Project Management Plan Updates	C.4.1.4	As project changes occur, such as issuing of TDLs, within 10 workdays (no less frequently than annually)	UR
10	Trip Report(s)	C.4.1.5	Within MSR report as an attachment following completion of each	UR

			trip.	
11	Draft Baseline Quality Control Plan	C.4.1.6	Submitted within 10 workdays of PS.	UR
12	Final Baseline Quality Control Plan	C.4.1.6	10 workdays after receipt of Government comments	UR
13	Quality Control Plan Updates	C.4.1.6	As project changes occur, such as issuing of TDLs, within 10 workdays (no less frequently than annually)	UR
14	Monthly Financial Reporting	C.4.1.7	Submitted monthly 5 workdays prior to technical status meeting.	UR
15	Supplemental Financial Reporting	C.4.1.7	Submitted monthly 5 workdays prior to technical status meeting.	UR
16	Presentation Materials	C.4.1.8	5 workdays after presentation	
17	Draft Transition-Out Plan	C.4.1.9	Within six months of PS	UR
18	Final Transition-Out Plan	C.4.1.9	10 workdays after receipt of Government comments	UR
19	Transition-Out Plan Updates	C.4.1.9	Annually and then quarterly during final Option Period.	UR
20	Transition-Out Plan Implementation	C.4.1.9	3 months prior to contract expiration date	UR
21	Labor Hours Report	C.4.1.10	Annually	UR
22	Infrastructure Development Plan	C.4.2.5	Required as specified in applicable TDLs	UR
23	Design results, artifacts, and documentation	C4.2.5	Required as specified in applicable TDLs	UR
24	Results, artifacts, and documentation	C.4.2.6	Required as specified in applicable TDLs	UR
25	Results, artifacts, and	C.4.2.7	Required as	UR

	documentation		specified in applicable TDLs	
26	After Action Reviews (AAR)	C.4.2.8	Within 5 days of completion of applicable integration support	UR
27	Technical documentation and reports	C4.2.8	Required as specified in applicable TDLs	UR
28	Test and evaluation analysis and reporting	C.4.2.9	Required as specified in applicable TDLs	UR
29	Copy of TO (initial award and all modifications)	N/A	Within 10 workdays of award	N/A
30	Documentation, presentations, visualizations, and other training coursework	C.4.3.3	Required as specified in applicable TDLs	UR

*UR = Unlimited Rights